

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

EMILY HEERDE, *et al.*,
Plaintiffs,
v.
LEARFIELD COMMUNICATIONS,
LLC, *et al.*,
Defendants.

Case No. 2:23-cv-04493-FLA (MAAx)

**ORDER GRANTING IN PART AND
DENYING IN PART DEFENDANTS'
MOTION TO DISMISS [DKT. 38]**

RULING

Before the court is Defendants Learfield Communications, LLC and Sidearm Sports, LLC’s (jointly, “Defendants” or “Learfield”)¹ Motion to Dismiss the Complaint (“Motion”). Dkt. 38-1 (“Mot.”). Plaintiffs Emily Heerde and Mark Haines (jointly, “Plaintiffs”) oppose the Motion. Dkt. 43 (“Opp’n”).

On November 28, 2023, the court found this matter appropriate for resolution without oral argument and vacated the hearing set for December 1, 2023. Dkt. 56; *see* Fed. R. Civ. P. 78(b); Local Rule 7-15. For the reasons stated below, the Motion is GRANTED IN PART and DENIED IN PART.

BACKGROUND

Plaintiffs bring this putative class action on behalf of all persons who visited the website www.usctrojans.com (“Trojans Website”) or any college athletics website operated by Defendants (“Team Websites”) and either: (i) subscribed to e-newsletters from the Team Websites before watching pre-recorded videos on the Team Websites; or (ii) used search bars built into the Team Websites (“Search Bars”). Dkt. 1 (“Compl.”) ¶ 1.

The first putative class relates to Defendants’ implementation of the Facebook Pixel (“Pixel”) on the Team Websites. *See id.* ¶ 5; Opp’n at 1. Plaintiffs and the class members allegedly requested and watched videos on the Team Websites, and the Pixel caused their web browsers to transfer their Facebook IDs and information about the videos they requested (*e.g.*, their titles) to Facebook in violation of the Video Privacy Protection Act (“VPPA”), 18 U.S.C. § 2710, *et seq.* Compl. ¶¶ 5, 14, 26, 347–48; *see also* Opp’n at 1.

The second putative class relates to Defendants’ implementation of Search Bars powered by Google on the Team Websites. *See* Compl. ¶¶ 6–7; Opp’n at 1–2.

¹ Learfield Communications, LLC and Sidearm Sports, LLC refer to themselves jointly as “Learfield.” Dkt. 38-1 at 1.

1 Plaintiffs and the class members allegedly entered search terms into the Search Bars
2 (“Search Terms”) to search for content on the Team Websites, and believed their
3 Search Terms were being sent solely to the owners of the Team Websites (*e.g.*, the
4 University of Southern California (“USC”)). Compl. ¶¶ 6–7. Plaintiffs, however,
5 allege their Search Terms were simultaneously fed to Defendants and other third
6 parties—specifically, Google, Meta, Oracle, The Trade Desk, and comScore
7 (collectively, the “tracking entities” or “Third Parties”)—in violation of the California
8 Invasion of Privacy Act (“CIPA”), Cal. Penal Code §§ 631, 635, the Federal Wiretap
9 Act, 18 U.S.C. § 2510, *et seq.*, and their privacy rights under the California
10 Constitution. Compl. at 1–2; *id.* ¶ 27; *see also* Opp’n at 1–2.

11 On June 8, 2023, Plaintiffs filed a Complaint against Defendants and USC. *See*
12 Compl. On September 6, 2023, Plaintiffs and USC jointly stipulated to USC’s
13 dismissal without prejudice. Dkt. 35. On September 21, 2023, Defendants filed the
14 instant Motion, seeking dismissal of all claims pursuant to Rules 12(b)(6) and
15 12(b)(7). *See* Mot. On November 9, 2023, Defendants filed a Motion to Stay
16 Discovery Pending Resolution of the Motion to Dismiss (“Motion to Stay
17 Discovery”). Dkt. 45. Defendants also filed several notices of supplemental
18 authorities. *See* Dkts. 61, 64, 68, 71, 73, 74, 78, 79, 80, 81, 82.

19 Notably, Defendants cite three cases brought by Plaintiffs’ counsel against
20 Defendants in other districts, and contain similar allegations to those in the instant
21 matter. *See Peterson v. Learfield Commc’ns, LLC*, Case No. 8:23-cv-146-BCB
22 (MDNx), 2023 WL 9106244 (D. Neb. Dec. 8, 2023); *Edwards v. Learfield Commc’ns,*
23 *LLC*, Case No. 1:23-cv-65-AW (MAFx), 2023 WL 8544765 (N.D. Fla. Oct. 6, 2023);
24 *NTS; Brown v. Learfield Commc’ns, LLC*, Case No. 1:23-cv-00374-DAE, 2024 WL
25 1477636 (W.D. Tex. Jan. 29, 2024). The courts in each of these districts dismissed
26 the VPPA claims. *See id.*

FAILURE TO STATE A CLAIM

I. Legal Standard

Under Rule 12(b)(6), a party may file a motion to dismiss a complaint for “failure to state a claim upon which relief can be granted.” The purpose of Rule 12(b)(6) is to enable defendants to challenge the legal sufficiency of the claims asserted in the complaint. *Rutman Wine Co. v. E. & J. Gallo Winery*, 829 F.2d 729, 738 (9th Cir. 1987). A district court properly dismisses a claim under Rule 12(b)(6) if the complaint fails to allege sufficient facts “to state a cognizable legal theory or fails to allege sufficient factual support for its legal theories.” *Caltex Plastics, Inc. v. Lockheed Martin Corp.*, 824 F.3d 1156, 1159 (9th Cir. 2016).

“To survive a motion to dismiss, a complaint must contain sufficient factual matter ... to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). “While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, a plaintiff’s obligation to provide the ‘grounds’ of his ‘entitlement to relief’ requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” *Twombly*, 550 U.S. at 555 (citations and brackets omitted).

“Factual allegations must be enough to raise a right to relief above the speculative level on the assumption that all the allegations in the complaint are true (even if doubtful in fact).” *Id.* (citations and parentheticals omitted). “Determining whether a complaint states a plausible claim for relief is ‘a context-specific task that requires the reviewing court to draw on its judicial experience and common sense.’” *Ebner v. Fresh, Inc.*, 838 F.3d 958, 963 (9th Cir. 2016) (quoting *Iqbal*, 556 U.S. at 679).

When evaluating a complaint under Rule 12(b)(6), the court “must accept all well-pleaded material facts as true and draw all reasonable inferences in favor of the plaintiff.” *Caltex*, 824 F.3d at 1159. Legal conclusions “are not entitled to the

1 assumption of truth” and “must be supported by factual allegations.” *Iqbal*, 556 U.S.
2 at 679. The court need not accept as true allegations that contradict matters properly
3 subject to judicial notice or established by exhibits attached to the complaint.
4 *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001), *amended on*
5 *other grounds*, 275 F.3d 1187 (9th Cir. 2001). “Nor is the court required to accept as
6 true allegations that are merely conclusory, unwarranted deductions of fact, or
7 unreasonable inferences.” *Id.*

8 **II. VPPA – 18 U.S.C. § 2710, *et seq.***

9 “The impetus for [the VPPA] occurred when a weekly newspaper in
10 Washington published a profile of Judge Robert H. Bork based on the titles of 146
11 films his family had rented from a video store.” Video Privacy Protection Act of
12 1988, S. Rep. No. 100-599, at 5. Its purpose is “[t]o preserve personal privacy with
13 respect to the rental, purchase, or delivery of video tapes or similar audio-visual
14 materials.” *Id.* at 1.

15 “The Act allows consumers to maintain control over personal information
16 divulged and generated in exchange for receiving services from video tape service
17 providers [and] reflects the central principle of the Privacy Act of 1974: that
18 information collected for one purpose may not be used for a different purpose without
19 the individual's consent.” *Id.* at 8. “Congress’s intent in passing the VPPA therefore
20 evinces the principle that protection is merited when the consumer lacks control over
21 the dissemination of the information at issue.” *Mollett v. Netflix, Inc.*, 795 F.3d 1062,
22 1065–66 (9th Cir. 2015).

23 The statute provides: “A video tape service provider [‘VTSP’] who knowingly
24 discloses, to any person, personally identifiable information [‘PII’] concerning any
25 consumer of such provider shall be liable to the aggrieved person,” unless the person
26 provides “informed, written consent.” 18 U.S.C. § 2710(b). To plead a plausible
27 claim under § 2710(b), a plaintiff must allege: “(1) a defendant is a ‘video tape service
28 provider,’ (2) the defendant disclosed ‘PII concerning any customer’ to ‘any person,’

(3) the disclosure was made knowingly, and (4) the disclosure was not authorized by § 2710(b)(2).” *Mollett*, 795 F.3d at 1066 (quotation marks in original).

All four elements are disputed here. Mot. at 11–18. Because Plaintiffs fail to allege sufficiently that their PII was disclosed, the court does not address Defendants’ other arguments at this time, including Defendants’ constitutional challenges to the VPPA. *See Camreta v. Greene*, 563 U.S. 692, 705 (2011) (“[A] longstanding principle of judicial restraint requires that courts avoid reaching constitutional questions in advance of the necessity of deciding them.”) (cleaned up).

A. “Personally Identifiable Information” (“PII”)

The VPPA defines PII to “include[] information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” 18 U.S.C. § 2710(a)(3). The Ninth Circuit has adopted an “ordinary person” standard to determine what constitutes PII under the VPPA: “[PII] means only that information that would readily permit an ordinary person to identify a specific individual's video-watching behavior.” *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 985 (9th Cir. 2017) (citations and quotation marks omitted).

In *Eichenberger*, a plaintiff insufficiently alleged a defendant disclosed PII where the defendant allegedly disclosed the serial number of plaintiff’s Roku box (a device that enables video streaming) and the names of videos he watched. *Id.* at 895–96. The serial number did not enable an “ordinary person” to identify the plaintiff because it created a “sizable pool of possible viewers.” *Id.* at 985. Only a more sophisticated person, such as a “resourceful private investigator” or a company with complex algorithms and access to “an enormous amount of information,” would be able to identify the plaintiff based solely on the serial number. *Id.* at 985–86. The Ninth Circuit, however, recognized that “modern technology may indeed alter—or may already have altered—what qualifies under the statute.” *Id.* at 986. “A Facebook link or an email address may very well readily enable an ‘ordinary person’ to identify an individual.” *Id.*

1 Plaintiffs allege the Pixel disclosed their PII; specifically, the Pixel disclosed
2 their Facebook user-IDs (“FIDs”) and video-watching data. *See* Compl. ¶¶ 141–159.
3 Plaintiffs allege FIDs “can be used, by anyone, to easily identify a Facebook user ...
4 by simply appending the [FID] to www.facebook.com (e.g.,
5 [www.facebook.com/\[FID_here\]](http://www.facebook.com/[FID_here])).” *Id.* ¶¶ 139–40. “That step ... direct[s] the browser
6 to the profile page, and all the information contained in or associated with the profile
7 page, for the user associated with the particular [FID].” *Id.* Plaintiffs allege their
8 video-watching data consists of: (1) requested URLs which identify the type of
9 content searched for (e.g., <https://hopkinssports.com/sports/mens-lacrosse-schedule>),
10 Compl. ¶¶ 146–49, and (2) metadata containing the title of a video (e.g., “Pac-12
11 Mental Health – University of Southern California”), *id.* ¶¶ 150–56.

12 Most courts have found the Pixel discloses PII at the pleading stage, at least
13 where plaintiffs also allege personal information existed on their Facebook page that
14 could be used to readily identify them. *See Ghanaat v. Numerade Labs, Inc.*, Case
15 No. 4:23-cv-00833-YGR, 2023 WL 5738391, at *4 (N.D. Cal. Aug. 28, 2023) (“Most,
16 if not all, courts to address the question [whether FIDs and URLs are PII] have found
17 at the pleading stage that [FIDs] are PII.”). Thus, *Ghanaat* “agree[d] an FID can
18 constitute PII where it leads to a Facebook page that discloses personal and
19 identifying information about the consumer,” but dismissed the VPPA claim with
20 leave to amend “because [plaintiffs] d[id] not allege their Facebook pages contain[ed]
21 any personal information, such as their names or email addresses.” 2023 WL
22 5738391, at *4.

23 In *Feldman v. Star Trib. Media Co. LLC*, 659 F. Supp. 3d 1006, 1020–21 (D.
24 Minn. 2023), a plaintiff plausibly alleged his PII was disclosed by the Pixel on a
25 defendant’s website when he also claimed that his Facebook profile contained his
26 name, “making it feasible to identify [him] by reference to this information.” *See also*
27 *Jackson v. Fandom, Inc.*, Case No. 22-cv-04423-JST, 2023 WL 4670285, at *4 (N.D.
28 Cal. July 20, 2023) (finding PII plausibly alleged where a plaintiff claimed that “a

1 user's Facebook profile may contain the user's name, gender, birthday, place of
2 residence, career, educational history, a multitude of photos, and the content of a
3 Facebook user's posts.") (internal quotation marks omitted).

4 This court holds that a person's FID can be used to identify that person if the
5 person's Facebook profile is publicly accessible and includes sufficient identifying
6 information. *See id.* (sufficient identifying information may include name, gender,
7 birthday, place of residence, career, education history, photographs, and content of
8 posts); *Control who can see your Facebook page*, Facebook,
9 <https://www.facebook.com/help/150193685051184/> (private profiles may not be
10 viewable even if someone has the FID).²

11 Here, Plaintiffs fail to allege their PII was disclosed because they do not
12 identify what information on their Facebook pages, if any, was viewable and could be
13 used to identify them. *See* Compl. ¶¶ 139–40. Thus, the Motion is GRANTED as to
14 Plaintiffs' VPPA claim. The VPPA claim is DISMISSED with twenty-one (21) days'
15 leave to amend.

16 **III. CIPA – Cal. Penal Code § 631**

17 “CIPA prohibits any person from using electronic means to learn the contents
18 or meaning of any communication without consent or in an unauthorized manner.” *In*
19 *re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 607 (9th Cir. 2020) (cleaned
20 up). Specifically, Cal. Penal Code § 631 (“§ 631”) creates four avenues for relief:

21 (1) where a person “by means of any machine, instrument, or
22 contrivance, or in any other manner, intentionally taps, or makes any
23 unauthorized connection ... with any telegraph or telephone wire, line,
cable, or instrument”;

24 (2) where a person “willfully and without consent of all parties to the
25 communication, or in any unauthorized manner, reads, or attempts to
26

27 ² The court takes judicial notice of this webpage. *See Lee v. City of Los Angeles*, 250
28 F.3d 668, 689 (9th Cir. 2001).

1 read, or to learn the contents or meaning of any message, report, or
2 communication while the same is in transit”;

3 (3) where a person “uses, or attempts to use, in any manner, or for any
4 purpose, or to communicate in any way, any information so obtained”;
5 and

6 (4) where a person “aids, agrees with, employs, or conspires with any
7 person or persons to unlawfully do, or permit, or cause to be done any of
8 the acts or things mentioned above.”

9 *Javier v. Assurance IQ, LLC*, 649 F.Supp.3d 891, 897 (N.D. Cal. 2023) (quoting Cal.
10 Penal Code § 631).

11 “Any person who has been injured by a violation of this chapter may bring an
12 action against the person who committed the violation” Cal. Penal Code § 637.2.
13 The analysis for a violation of CIPA is the same as under the Federal Wiretap Act.
14 *See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020); *Saleh v. Nike,*
15 *Inc.*, 562 F. Supp. 3d 503, 517 (C.D. Cal. 2021); *Facebook*, 956 F.3d at 607.

16 Plaintiffs allege essentially two theories.³ First, under the second clause of
17 § 631, Defendants intercepted their Search Terms which were intended for the owners
18 of the Team Websites (*e.g.*, USC), and not Defendants. Compl. ¶ 367; Opp’n at 11–
19 12. Second, under the fourth clause, Defendants aided and conspired with the tracking
20 entities to intercept the Search Terms because Defendants installed the Search Bars on
21 the Team Websites and knew the Search Terms would be sent to the tracking entities.
22 Compl. ¶¶ 6, 370; *see also* Opp’n at 1–2.

23 Defendants argue Plaintiffs fail to state a claim under § 631 for six reasons:
24 (1) Plaintiffs had no reasonable expectation of privacy in their communications;

25 ³ Plaintiffs appear to allege Defendants violated the first, second, and fourth clauses.
26 Compl. ¶¶ 365, 367, 370. The first clause, however, is not relevant because it
27 “concerns telephonic wiretapping specifically, which does not apply to the context of
28 the internet.” *Williams v. What If Holdings, LLC*, Case No. 22-cv-03780-WHA, 2022
WL 17869275, at *2 (N.D. Cal. Dec. 22, 2022) (citations omitted). The second and
fourth clauses are applicable to the Internet. *See id.*

(2) the “contents” of communications were not disclosed; (3) Defendants did not intercept any communications because they were a party to the communications rather than a third-party eavesdropper; (4) Plaintiffs consented to disclosure of their communications to Facebook; (5) Defendants did not intercept any communications while they were “in transit”; and (6) Defendants did not “read” the contents of any communications while the communications were in transit. Mot. at 20–27; Dkt. 46 (“Reply”) at 14–17. The court addresses each in turn.

A. Reasonable Expectation of Privacy

Defendants first argue “Plaintiffs do not have a reasonable expectation of privacy in the browsing information that was sent by the Pixel to the Third Parties,” Mot. at 21, and the issue “turns on whether [they allegedly] disclosed PII or statutorily protected information,” Reply at 21. Defendants, however, address only “browsing information” and “PII,” *see id.*, and fail to address the Search Terms, *see* Mot. at 21; Reply at 16; *see also* Compl. ¶¶ 6–7, 19–21; Opp’n at 14.

In any case, users have a reasonable expectation of privacy in “unique search terms.” *Brown v. Google LLC*, Case No. 4:20-cv-3664-YGR, 2023 WL 5029899, at *20 (N.D. Cal. Aug. 7, 2023) (“Ninth Circuit law indicates [] users [have a reasonable expectation of privacy] over URLs that disclose either unique search terms or the particular document within a website that a person views.”) (quotation marks and citation omitted); *see also infra* § [V.A](#) (finding Plaintiffs’ have a reasonable expectation of privacy in their Search Terms in the context of Plaintiffs’ claim for invasion of privacy).

Plaintiffs, therefore, allege plausibly a reasonable expectation of privacy in their communications.

B. “Contents” of Communications

Next, Defendants argue the Search Terms do not constitute “contents” of communications. Mot. at 21–23. The court disagrees. The Federal Wiretap Act defines “contents” to “include[] any information concerning the substance, purport, or

1 meaning of [a] communication.” 18 U.S.C. § 2510(8); *see also Yoon v. Lululemon*
2 *USA, Inc.*, 549 F. Supp. 3d 1073, 1082 (explaining this definition is applicable to
3 CIPA claims). “The term ‘contents’ refers to the intended message conveyed by the
4 communication, and does not include record information regarding the characteristics
5 of the message that is generated in the course of the communication.” *In re Zynga*
6 *Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014); *see also Yoon*, 549 F. Supp. 3d
7 at 1082 (explaining CIPA protects “user-generated material” but not “routine
8 identifiers”). Search terms constitute “contents” of a communication. *See Zynga*, 750
9 F.3d at 1108–09 (explaining URL data may contain “contents” of a communication if
10 a user’s search terms are included therein); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d
11 1051, 1083 (N.D. Cal. 2015) (finding search terms implicate “content”). Plaintiffs,
12 therefore, allege plausibly “contents” of communications.

13 C. Party Exception

14 Defendants argue the “party exception” shields them from liability because they
15 were parties to the communications—not third-party eavesdroppers. Mot. at 23
16 (quoting *Licea v. Vitacost.com, Inc.*, Case No. 22-cv-1854-RSH (WVGx), 2023 WL
17 5086893, at *3 (S.D. Cal. July 24, 2023) (“A party to a conversation is not liable
18 under [§] 631(a) for recording its own conversation.”)). Plaintiffs counter the party
19 exception applies only where a defendant is the “known and intended recipient” of a
20 plaintiff’s communications. Opp’n at 12 (quoting *Peña v. GameStop, Inc.*, 670 F.
21 Supp. 3d 1112, 1118 (S.D. Cal. 2023). “[A]s far as Plaintiffs and other subscribers
22 were aware, the Website was run by USC.” Opp’n at 11–12. The court agrees with
23 Plaintiffs.

24 1. Legal Standard

25 “Two basic principles of Section 631 liability are undisputed.” *Javier*, 649 F.
26 Supp. 3d at 897. “First, if a third party listens in on a conversation between the
27 participants (even if one participant consents to the presence of that third party), then
28 the third party is liable under the second prong (and the participant is often liable

1 under the fourth prong).” *Id.* at 897–98 (citing *Ribas v. Clark*, 38 Cal. 3d 355, 359–62
2 (1985) (party exception did *not* apply where one spouse (the wife) asked a defendant
3 to listen in to a conversation with her husband)). “[S]uch secret monitoring denies the
4 speaker an important aspect of privacy of communication—the right to control the
5 nature and extent of the first-hand dissemination of his statements.” *Ribas*, 38 Cal. 3d
6 at 361.

7 “Second, a party to a conversation can record it without the other party’s
8 knowledge without incurring [§] 631 liability.” *Javier*, 649 F. Supp. 3d at 898 (citing
9 *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 897–99 (1975) (party exception applied where
10 a defendant used a tape recorder to record a telephone conversation and later played
11 the conversation for a third party, because “[i]t is never a secret to one party to a
12 conversation that the other party is listening to the conversation; only a third party can
13 listen secretly to a private conversation.”)). “While one who imparts private
14 information risks the betrayal of his confidence by the other party, a substantial
15 distinction has been recognized between the secondhand repetition of the contents of a
16 conversation and its simultaneous dissemination to an unannounced second auditor,
17 whether that auditor be a person or mechanical device.” *Ribas*, 38 Cal. 3d at 360–61
18 (citation omitted).

19 This court previously found that, when an internet user knowingly
20 communicates with a website owner, the website owner is a party to the
21 communication. *Saleh*, 562 F. Supp. 3d at 519. But there is a split among courts
22 regarding how to apply *Rogers* and *Ribas* to communications between internet users
23 and developers of websites who track or record user data. *See Yockey v. Salesforce,*
24 *Inc.*, Case No. 22-cv-09067-JST, 2023 WL 5519323, at *3–5 (N.D. Cal. Aug. 25,
25 2023). While one set of courts consider a software developers’ *intentions* with respect
26
27
28

1 to the use of the collected information,⁴ others contend the proper question is whether
2 a developer has the *capability* to use the information for any purpose other than to
3 furnish the communications to the website owner.⁵ *Yockey*, 2023 WL 5519323, at *5
4 (citing *Javier*, 649 F. Supp. 3d at 900).

5 *Javier* and *Yockey* disagreed with the former courts' reading for two reasons.
6 First, that group "interpret[ed] the second prong of the statute ... based on the
7 intentions and usage of the prospective third party," "[b]ut the third prong of the
8 statute already penalizes 'use.'" *Javier*, 649 F. Supp. 3d. at 900. As a result, "reading
9 a use requirement into the second prong would add requirements that are not present
10 (and swallow the third prong in the process)." *Id.* Second, the California Supreme
11 Court in *Ribas* did not consider the intention of the eavesdropper, but rather
12 "emphasized the privacy concerns at issue with having an 'unannounced second
13 auditor' listening in on the call," which implicates an individual's "right to control the
14 nature and extent of the firsthand dissemination of [their] statements." *Id.* (quoting
15 *Ribas*, 38 Cal. 3d at 360–61).

16 This court agrees with the reasoning of *Yockey* and *Javier* and finds a third
17 party's intent with respect to the use of the collected information is irrelevant. The
18 inquiry turns on whether the third party has the capability to use the communications
19 for any purpose other than to provide those communications to the intended recipient.⁶
20

21 ⁴ See *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 832 (N.D. Cal. 2021); *Williams*,
22 2022 WL 17869275, at *3; *Johnson v. Blue Nile, Inc.*, Case No. 20-cv-08183-LB,
23 2021 WL 1312771, at *3 (N.D. Cal. Apr. 8, 2021); *Yale v. Clicktale, Inc.*, Case No.
24 20-cv-07575-LB, 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021).

25 ⁵ See *Facebook*, 956 F.3d at 608; *Revitch v. New Moosejaw, Inc.*, Case No. 18-cv-
26 06827-VC, 2019 WL 5485330, at *1 (N.D. Cal. Oct. 2023); *Saleh*, 562 F. Supp. 3d
at 521; *Yoon*, 549 F. Supp. 3d at 1081.

27 ⁶ Even if a defendant's intent were relevant to the party exception analysis, Plaintiffs
28 allege sufficiently Defendants' intent to share their communications with third parties

1 **2. Discussion**

2 *a. Second clause of § 631*

3 Defendants argue they were parties to the communications because, under
4 Plaintiffs’ own allegations, they were the *de facto* website owners. Reply at 16.
5 Plaintiffs allege “there is no aspect of the websites run by the Operator Defendants
6 that is controlled by the college, university, or team itself,” and “USC has completely
7 relinquished control to the Operator Defendants and allowed them to run the Trojans
8 Website without oversight.” *Id.* (quoting Compl. ¶ 90).

9 The court disagrees that Defendants were parties to the communications.
10 Plaintiffs allegedly believed that, when they entered their Search Terms, the Search
11 Terms would be sent to the Teams, not to Defendants. Compl. ¶ 204. This case,
12 therefore, is distinguishable from *Saleh*, where plaintiffs believed their
13 communications were being received by the website owner, and the website owner
14 properly claimed the party exception. 562 F. Supp. 3d at 519.

15 Plaintiffs’ beliefs as to whom they are communicating with is critical to what
16 § 631 seeks to protect—unknown disclosure to “an unannounced second auditor.”
17 *Ribas*, 38 Cal. 3d. at 360–61. Here, Defendants are the alleged “unannounced second
18 auditor.” See Compl. ¶¶ 196–98 (alleging the Search Bars provide no indication they
19 are associated with Defendants or any tracking entity), 316 (“USC was the intended
20 recipient of Plaintiffs’ communications ... The Operator Defendants re-routed
21 Plaintiffs’ Search Terms, along with those for all users and subscribers to the Trojans
22 Website, meant for USC, to Google ...”). Thus, Plaintiffs allege plausibly Defendants
23 were third-party eavesdroppers to Plaintiffs’ communications.

24
25
26

27 for profit. See Compl. ¶ 205 (“The Operator Defendants choose to monetize the
28 search results provided by the [Search Bar] by including ads as well as sharing the
 Search Terms with tracking entities.”).

1 *b. Fourth clause of § 631*

2 Plaintiffs have also alleged sufficiently Defendants violated the fourth clause by
3 aiding and conspiring with third-party tracking entities to intercept Plaintiffs’ search
4 terms. It is undisputed the party exception does not apply to the tracking entities. *See*
5 Reply at 14–16. Plaintiffs allege Defendants aided and conspired with the tracking
6 entities to intercept Plaintiffs’ search terms because Defendants: (1) added the Search
7 Bars to the Team Websites; (2) hid attribution to Google; and (3) otherwise did not
8 notify Plaintiffs their search terms would be sent to the tracking entities. Compl.
9 ¶¶ 180–206. As the party exception does not shield Defendants from liability,
10 Plaintiffs’ pleading is sufficient in this regard.

11 **D. Consent to Disclose to Facebook**

12 “Under the Wiretap Act, the question of express consent is usually a question of
13 fact, where a fact-finder needs to interpret the express terms of any agreements to
14 determine whether these agreements adequately notify individuals regarding the
15 interceptions.” *Matera v. Google Inc.*, Case No. 15-cv-04062-LHK, 2016 WL
16 5339806, at *17 (N.D. Cal. Sept. 23, 2016) (quotation marks and citations omitted).
17 While the parties dispute who has the burden to show consent, Opp’n at 15–16; Reply
18 at 16–17, district courts in the Ninth Circuit place the burden on Defendants, and this
19 court follows, *see, e.g., Matera*, 2016 WL 5339806, at *17; *Brown, v. Google LLC*,
20 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021); *see also In re Pharmatrak, Inc.*, 329
21 F.3d 9, 19 (1st Cir. 2003) (“We think, at least for the consent exception under the
22 [Wiretap Act] in civil cases, that it makes more sense to place the burden of showing
23 consent on the party seeking the benefit of the exception, and so hold.”).

24 Defendants contend Plaintiffs consented to having their Search Terms disclosed
25 to Facebook because they agreed to Facebook’s policies; thus, Plaintiffs purportedly
26 “consented to the communication of website usage information to Facebook.” Mot.
27 at 25; *see also id.* at 16–18; Reply at 17 (“It is implausible that Plaintiffs obtained
28 Facebook accounts without consenting to Facebook’s policies ...”). Defendants,

1 however, do not attach or seek judicial notice of Facebook’s policies, and, thus, fail to
2 show Plaintiffs unequivocally consented to Defendants’ alleged feeding of their
3 Search Terms to Facebook. *See* Mot. at 25. Additionally, Plaintiffs allege the “Team
4 Websites do not provide users” any “opportunity to consent to ... use of a Search Bar
5 [that] would cause their Search Terms to be shared with various parties.” Compl. ¶ 7.

6 Drawing all reasonable inferences in favor of Plaintiffs, Plaintiffs allege
7 plausibly they did not consent to their Search Terms being sent to Facebook.

8 **E. Intercepted in Transit**

9 For a communication to be “‘intercepted,’ it must be acquired during
10 transmission, not while it is in electronic storage.” *Konop v. Hawaiian Airlines, Inc.*,
11 302 F.3d 868, 878 (9th Cir. 2002). Defendants argue Plaintiffs “have not alleged any
12 facts that the Third Parties intercept[ed] communications before or at the same time
13 they are provided to [Defendants] on the Team Websites.” Mot. at 26. The court
14 disagrees. Plaintiffs allege that, after they entered their Search Terms, the Search
15 Terms were replicated and sent in parallel to the tracking entities. *See* Compl. ¶¶ 223,
16 234, 269, 276, 289, 296. Defendants’ other position hinges on their previous
17 argument that they are parties to the communications, and thus could not “intercept”
18 the communications. Mot. at 26; Reply at 16. The court rejected this argument. *See*
19 *supra* § III.C.2.

20 Therefore, Plaintiffs allege adequately that Defendants intercepted Search
21 Terms intended for the Team Websites and that their communications were
22 intercepted in transit. *See id.*; Compl. ¶¶ 6–7, 366 (“Plaintiff and members ... used
23 the search function to communicate Search Terms to USC, with the expectation of
24 receiving search results provided by USC.”).

25 **F. Attempt to Learn the Contents of Communications**

26 Defendants argue Plaintiffs fail “to allege any facts” that Defendants “read,”
27 “attempted to read,” or attempted to “learn the contents of any communication” while
28 it was “in transit.” Mot. at 216; *see* Cal. Penal Code § 631(a). Plaintiffs, however,

1 allege Defendants intercepted the Search Terms while they were in transit to the Team
2 Websites and redirected them to “statcollect.sidearmsports.com” so that they could be
3 utilized by Defendants. Compl. ¶¶ 289–90. Plaintiffs, thus, allege sufficiently
4 Defendants attempted to learn the contents of their communications.

5 **IV. CIPA – Cal. Penal Code § 635**

6 Plaintiffs allege Defendants violated Cal. Penal Code § 635 (“§ 635”), which
7 provides, in relevant part:

8 Every person who manufactures, assembles, sells, offers for sale,
9 advertises for sale, possesses, transports, imports, or furnishes to another
10 any device which is primarily or exclusively designed or intended for
eavesdropping upon the communication of another

11 As with Cal. Penal Code § 631(a), a private party may bring a claim for violation of
12 § 635 under § 637.2(a) if the party has been “injured by a violation of this chapter.”
13 Cal. Penal Code § 637.2(a).

14 Plaintiffs allege Defendants “possesse[d]” the Search Bar code or
15 “assemble[d]” the Search Bar code as part of their “Sidearm Pixel.” *See* Cal. Penal
16 Code § 635; Compl. ¶¶ 101 (alleging Defendants’ “Sidearm Pixel” monitors user
17 activity on the Team Websites), 289 (“The Sidearm Pixel [] intercepts a visitors’
18 Search Terms when using the Search Bar, as depicted below ...”), 376 (“[B]y
19 implementing its own Sidearm Pixel in addition to the tracking tools, Operator
20 Defendants intentionally manufactured, assembled, sold, offered for sale, advertised
21 for sale, possessed, transported, imported, and/or furnished a wiretap device that is
22 primarily or exclusively designed or intended for eavesdropping upon the
23 communication of another.”).

24 Plaintiffs, however, do not allege any “concrete” injury resulting from
25 Defendants’ possession or assembly of the purported eavesdropping devices, and,
26 thus, lack Article III standing. *See TransUnion LLC v. Ramirez*, 594 U.S. 413, 424
27 (2021) (Article III standing requires “the plaintiff’s injury in fact be concrete—that is,
28 real, and not abstract”) (citations and internal quotation marks omitted); *Saleh*, 562 F.

1 Supp. 3d at 522–24 (plaintiff lacked standing to assert claim under § 635 because
2 plaintiff did not allege concrete injury resulted from defendants’ mere possession of
3 eavesdropping device).⁷

4 The Motion, therefore, is GRANTED as to Plaintiffs’ § 635 claim. The § 635
5 claim is DISMISSED with twenty-one (21) days’ leave to amend.

6 **V. Invasion of Privacy Under the California Constitution**

7 To state a claim for invasion of privacy under the California Constitution, a
8 plaintiff must show: “(1) there exists a reasonable expectation of privacy; and (2) the
9 intrusion was highly offensive.” *Facebook*, 956 F.3d at 601 (citation omitted).
10 Plaintiffs allege their privacy was invaded each time they entered Search Terms
11 because they did not know their Search Terms were being fed to Defendants and the
12 tracking entities, rather than solely to the respective Team Website. Compl. ¶¶ 6–7,
13 27, 111–21, 209–13, 298–307, 403–07; *see also* Opp’n at 1–2. Defendants argue
14 Plaintiffs’ allegations are insufficient under both prongs of *Facebook*. *See* Mot. at 38;
15 Reply at 17–18. The court disagrees.

16 **A. Reasonable Expectation of Privacy**

17 “The existence of a reasonable expectation of privacy, given the circumstances
18 of each case, is a mixed question of law and fact.” *Facebook*, 956 F.3d at 601
19 (citation omitted). Courts consider a variety of factors in determining whether a
20 reasonable expectation of privacy exists, including the “customs, practices, and
21 circumstances surrounding a defendant’s particular activities.” *Id.* at 602. For
22 example, in *Facebook*, plaintiffs alleged plausibly a reasonable expectation of privacy
23 in their browsing data where defendant Facebook collected their browsing data even
24

25 ⁷ Although California case law recognizes Cal. Penal Code § 637.2 does not require a
26 plaintiff to show it “has suffered, or been threatened with actual damages” to bring
27 suit, *Ion Equip. Corp. v. Nelson*, 110 Cal. App. 3d 868, 882 (1980), “standing in
28 federal court is a question of federal law, not state law,” *Hollingsworth v. Perry*, 570
U.S. 693, 715 (2013).

1 after they logged out of Facebook, because they had “privacy interests” in their
2 browsing histories and other collected data, and because of “Facebook’s allegedly
3 surreptitious and unseen data collection.” *Id.* at 602–03; *see also id.* at 603 (“[B]oth
4 the nature of collection and the sensitivity of the collected information are
5 important.”).

6 Here, Plaintiffs allege plausibly a reasonable expectation of privacy in their
7 search terms. As pleaded, a reasonable factfinder could determine the Search Terms
8 were sensitive and confidential because they revealed the specific content Plaintiffs
9 consumed. *See id.*; *Brown*, 2023 WL 5029899, at *20 (“Ninth Circuit law indicates []
10 users [have a reasonable expectation of privacy] over URLs that disclose either unique
11 search terms or the particular document within a website that a person views.”)
12 (internal quotations marks and citation omitted); Compl. ¶¶ 207–13.

13 Additionally, Defendants allegedly collected the Search Terms surreptitiously,
14 which supports a finding of reasonable expectation of privacy. *See Facebook*, 956
15 F.3d at 603. In particular, Defendants purportedly made substantial efforts to conceal
16 attribution of the Search Bars to Google, Compl. ¶¶ 118–121, 184–98, and misled
17 Plaintiffs into believing they could search using Google but only after they searched
18 using the Search Bar, *id.* at 116–17. These facts sufficiently plead a reasonable
19 expectation of privacy.

20 **B. Intrusion Highly Offensive**

21 “Actionable invasions of privacy also must be highly offensive to a reasonable
22 person, and sufficiently serious and unwarranted so as to constitute an ‘egregious
23 breach of the social norms.’ *Facebook*, 956 F.3d at 606 (internal quotations marks
24 and citation omitted). “Determining whether a defendant's actions were highly
25 offensive to a reasonable person requires a holistic consideration of factors such as the
26 likelihood of serious harm to the victim, the degree and setting of the intrusion, the
27 intruder's motives and objectives, and whether countervailing interests or social norms
28 render the intrusion inoffensive.” *Id.* (internal quotation marks and citations omitted).

1 “While analysis of a reasonable expectation of privacy primarily focuses on the nature
2 of the intrusion, the highly offensive analysis focuses on the degree to which the
3 intrusion is unacceptable as a matter of public policy.” *Id.* “Whether [] conduct was
4 highly offensive can rarely be resolved at the pleading stage.” *In re Google RTB*
5 *Consumer Priv. Litig.*, 606 F. Supp. 3d 935, 946 (N.D. Cal. 2022).

6 Here, Defendants’ alleged interception of the Search Terms and feeding to the
7 tracking entities may constitute a highly offensive intrusion, and, thus, raises a
8 question that cannot be resolved on a motion to dismiss as a matter of law. *See*
9 *Facebook*, 956 F.3d at 606 (“The ultimate question of whether Facebook’s tracking
10 and collection practices could highly offend a reasonable individual is an issue that
11 cannot be resolved at the pleading stage.”). A reasonable factfinder could determine
12 the alleged surreptitious collection of and profiting from Search Terms across over
13 300 sports team websites was an unacceptable intrusion in violation of public policy.
14 *See Compl.* ¶¶ 74, 204–06; *Brown*, 2023 WL 5029899, at *20 (unable to conclude as a
15 matter of law that certain data collection “was not highly offensive” where plaintiffs
16 proffered evidence that the data collected was “vast and sensitive”).

17 C. Conclusion Regarding Invasion of Privacy

18 Plaintiffs allege adequately a cause of action for invasion of privacy under the
19 California Constitution. Defendant’s Motion, therefore, is DENIED as to this claim.

20 VI. Federal Wiretap Act – 18 U.S.C. § 2510, *et seq.*

21 Defendants repeat the same arguments regarding the Federal Wiretap Act that
22 they raised with respect to CIPA. *See Mot.* at 28–30. The analysis for a violation of
23 the Federal Wiretap act is the same as under CIPA. *See Brodsky*, 445 F. Supp. 3d
24 at 127; *Saleh*, 562 F. Supp. at 517; *Facebook*, 956 F.3d at 607. For the same reasons
25 stated above, Defendants’ Motion as to the Federal Wiretap Act is DENIED. *See*
26 *supra* §§ [III.C.2](#) (party exception), [III.D](#) (consent to disclose to Facebook), [III.B](#)
27 (“contents” of communication), [III.E](#) (intercepted in transit).
28

FAILURE TO JOIN AN INDISPENSABLE PARTY

I. Legal Standard

Under Rule 12(b)(7), a defendant may move to dismiss a complaint for failure to join a necessary party under Rule 19. Rule 19 imposes a three-step inquiry:

(1) Is the absent party necessary (i.e., required to be joined if feasible) under Rule 19(a)?

(2) If so, is it feasible to order that the absent party be joined?

(3) If joinder is not feasible, can the case proceed without the absent party, or is the absent party indispensable such that the action must be dismissed?

Salt River Project Agr. Imp. & Power Dist. v. Lee, 672 F.3d 1176, 1179 (9th Cir. 2012).

A party may be necessary under Rule 19(a) in three different ways. *Id.* First, a party is necessary if, in the party's absence, the court cannot accord complete relief among existing parties. Fed. R. Civ. P. 19(a)(1)(A). Second, a party is necessary if the party has an interest in the action and resolving the action in the party's absence may as a practical matter impair or impede the party's ability to protect that interest. Fed. R. Civ. P. 19(a)(1)(B)(i). Third, a party is necessary if the party has an interest in the action and resolving the action in the party's absence may leave an existing party subject to inconsistent obligations because of that interest. Fed. R. Civ. P. 19(a)(1)(B)(ii).

II. USC

Defendants argue the Complaint should be dismissed because USC is an indispensable party, but do not engage in the Rule 19 analysis. Mot. at 30. This is insufficient. *See* Local Rules 7-4–7-5. Defendants' Motion as to indispensable party, therefore, is DENIED. *See also Brown v. Learfield*, 2024 WL 1477636, at *3 (denying Defendants' argument that University of Texas was an indispensable party); *Edwards v. Learfield*, 2023 WL 8544765, at *4–5 (same regarding University of


Florida); *Peterson v. Learfield*, 2023 WL 9106244, at *9–10 (same regarding University of Nebraska).

CONCLUSION

For the foregoing reasons, the court GRANTS Defendants’ Motion (Dkt. 38) as to Plaintiffs’ claims pursuant to the VPPA (First Cause of Action) and Cal. Penal Code § 635 (Third Cause of Action), and DISMISSES those claims with twenty-one (21) days’ leave to amend. The court DENIES Defendants’ Motion as to Plaintiffs’ claims under Cal. Penal Code § 631 (Second Cause of Action), the Federal Wiretap Act (Fourth Cause of Action), and for invasion of privacy under the California Constitution (Fifth Cause of Action). The court DENIES Defendants’ Motion to Stay Discovery (Dkt. 45) as moot.

IT IS SO ORDERED.

Dated: July 19, 2024


FERNANDO L. AENLLE-ROCHA
United States District Judge